CLAIMS

1. A system for making a purchase transaction by PIN purchasing over the Internet comprising:

a merchant's check out web page on a merchant server for a buyer to make a purchase from the buyer's browser;

means for the buyer selecting PIN purchase as a payment method and for entering a debit card number;

an Internet authorization server to which the merchant system re-directs said buyer's browser and to which the merchant system passes along a unique transaction id coupled to said transaction;

means for said Internet authorization server displaying a secure PIN pad screen and using a unique session key;

an input device for the buyer to enters a PIN;

means for encrypting said using said unique session key;

a host security module to which said Internet authorization server passes said encrypted PIN, said host security module generating an encrypted ANSI PIN block;

means for said ANSI PIN block passing back to said Internet authorization server;

means for said Internet authorization server returning control of said buyer's browser to said merchant server and passing along said unique transaction id;

a payment request based on contents of a shopping cart and said payment method, wherein said payment request is created by said merchant server;

an Internet payments server to which said merchant server sends said payment request, wherein said Internet payments server determines said payment type and formats a payment authorization request;

an ATM/POS system to which said payment authorization request is routed, wherein said ATM/POS system takes said encrypted ANSI PIN block passed along with said payment request and routes said ANSI PIN block through a second host secure module to be decrypted and translated;

a data deposit account system wherein if said transaction is an on-us transaction, then said ATM/POS system validates said PIN and passes a transaction amount coupled to said transaction to said associated data deposit account system for authorization;

a network coupled to the buyer's issuing financial institution, wherein if said transaction is an off-us transaction, then said authorization request is routed to said network to be further routed to said buyer's issuing financial institution;

means for passing back to said ATM/POS system and finally back to said merchant server an authorization approval or denial.

2. The system of Claim 1, wherein said unique session is under Secure Sockets Layer (SSL) technology.

3. The system of Claim 1, wherein a link between said Internet authorization server and said Internet payments server is a secure link.

4. The system of Claim 1, wherein said means for encrypting a user's PIN further comprises:

means for an Internet authorization server receiving control of a browser of said user from a merchant server, and receiving data comprising: merchant id, transaction id, return URL, and a merchant defined as its own entity and which does not contain the user's PIN;

means for said Internet authorization server initiating a call to a host secure module to request a public key, PubK;

means for said host secure module returning PubK + Slot;

means for said Internet authorization server passing JavaScript and PubK back to said browser;

means for said user entering and submitting a PIN, wherein digits are hidden;

means for generating a DES key, KD at said browser;

means for encrypting said entered PIN digits using KD(PIN);

means for encrypting KD using PubK;

means for posting KD(PIN) + PubK(KD) to said IAS;

means for said Internet authorization server passing said KD(PIN) + PubK(KD) + Slot to said host secure module;

means for said host secure module converting said KD(PIN) + PubK(KD) + Slot to MFK(KPE) + KPE(PIN), wherein such conversion is used to create a standard ANSI PIN block;

means for said host secure module passing said MFK(KPE) + KPE(PIN) back to said IAS; and

means for said Internet authorization server storing said MFK(KPE) + KPE(PIN) + Transaction Id + a timestamp in a database.

5. A method for making a purchase transaction by PIN purchasing over the Internet, said method comprising the steps of:

a buyer proceeding to a merchant's checkout page on a merchant server from a buyer's browser to make a purchase;

said buyer selecting PIN Purchase as a payment method and entering an associated debit card number;

said merchant server re-directing said buyer's browser to an Internet authorization server and passing a unique transaction id coupled to said transaction;

said Internet authorization server displaying a secure PIN pad screen and using a unique session key;

said buyer entering said PIN using an input device;

encrypting said PIN using said unique session key;

said Internet authorization server passing said encrypted PIN to a host secure module, wherein said host secure module generates an associated encrypted ANSI PIN block;

said Internet authorization server returning control of said buyer's browser to said merchant server along with said unique transaction id;

said merchant server creating a payment request based on contents of said shopping cart and said payment method, wherein said merchant server sends said payment request to an Internet payments server;

said Internet payments server determining a payment type and formatting a payment authorization request;

said payment authorization request routing to an ATM/POS system, wherein said ATM/POS system takes said encrypted ANSI PIN block and routes it through a second host secure module to be decrypted and translated to an acquiring financial institution's encrypted PIN data;

if said transaction is on-us, then said ATM/POS system validating said PIN and passing an associated transaction amount to a data deposit account system for authorization;

if said transaction is off-us, then said authorization request routing to a network for routing to an issuing financial institution of said buyer;

passing back to said ATM/POS system an authorization approval or denial, wherein said authorization approval or denial is routed to said Internet payments server and finally back to said merchant server.

6. The method of Claim 5, wherein said unique session is under Secure Sockets Layer (SSL) technology.

7. The method of Claim 5, wherein a link between said Internet authorization server and said Internet payments server is a secure link.

8. The method of Claim 5, wherein encrypting a user's PIN further comprises the steps of:

an Internet authorization server receiving control of a browser of said user from a merchant server, and receiving data comprising: merchant id, transaction id, return URL, and a merchant defined as its own entity and which does not contain the user's PIN;

said Internet authorization server initiating a call to a host secure module to request a public key, PubK;

said host secure module returning PubK + Slot;

said Internet authorization server passing JavaScript and PubK back to said browser;

said user entering and submitting a PIN, wherein digits are hidden;

generating a DES key, KD at said browser;

encrypting said entered PIN digits using KD(PIN);

encrypting KD using PubK;

posting KD(PIN) + PubK(KD) to said IAS;

said Internet authorization server passing said KD(PIN) + PubK(KD) + Slot to said host secure module;

said host secure module converting said KD(PIN) + PubK(KD) + Slot to MFK(KPE) + KPE(PIN), wherein such conversion is used to create a standard ANSI PIN block;

said host secure module passing said MFK(KPE) + KPE(PIN) back to said IAS; and

said Internet authorization server storing said MFK(KPE) + KPE(PIN) + Transaction Id + a timestamp in a database.